NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EVALUATION OF U.S. NAVY SURFACE SHIP OPERATIONS IN THE INFORMATION DOMAIN

by

Crystal L. Sargent

March 2013

Thesis Advisor:	Steven J. Iatrou
Second Reader:	Deidre McLay

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE EVALUATION OF U.S. NAVY SURFACE SHIP OPERATIONS IN THE INFORMATION DOMAIN	**5. FUNDING NUMBERS**
6. AUTHOR(S) Crystal L. Sargent	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A_____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This addresses the current configuration of surface naval vessels for employment in the information domain. It will address how surface assets such as the Aegis Guided Missile Cruiser (CG) and Destroyer (DDG) fit into the modern era of naval information dominance.

An evaluation of past experiences and current technology will be used to recommend how to employ current surface assets information operations (IO) capabilities

This thesis will also include an evaluation of current topics regarding information Dominance and the cyber domain, focusing on the areas of electronic warfare, cyber warfare, and military information support operations (MISO).

14. SUBJECT TERMS Surface Ship, Cyber, Information Dominance, Information Operations (IO), Long Range Acoustic Device (LRAD), Fire Scout, Electronic Warfare, Military Information Support Operations (MISO)	**15. NUMBER OF PAGES** 81
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

EVALUATION OF U.S. NAVY SURFACE SHIP OPERATIONS IN THE INFORMATION DOMAIN

Crystal L. Sargent
Lieutenant, United States Navy
B.S, Jacksonville University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Author: Crystal L. Sargent

Approved by: Steven J. Iatrou
Thesis Advisor

CAPT Deidre McLay, USN
Second Reader

Dr. Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This addresses the current configuration of surface naval vessels for employment in the information domain. It will address how surface assets such as the Aegis Guided Missile Cruiser (CG) and Destroyer (DDG) fit into the modern era of naval information dominance.

An evaluation of past experiences and current technology will be used to recommend how to employ current surface assets information operations (IO) capabilities

This thesis will also include an evaluation of current topics regarding information dominance and the cyber domain, focusing on the areas of electronic warfare, cyber warfare, and military information support operations (MISO).

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIEWS	Advanced Integrated Electronic Warfare System
C2	Command and Control
DoD	Department of Defense
IDC	Information Dominance Corps
C10F	Commander Tenth Fleet
USNA	United States Naval Academy
NPS	Naval Postgraduate School
IO	Information Operations
ID	Information Dominance
PQS	Personal Qualification Standards
CG	Guided Missile Cruiser
DDG	Guided Missile Destroyer
CV/CVN	Air Craft Carrier
LHA	Landing Helicopter Assault
LHD	Landing Helicopter Dock
FFG	Guided Missile Frigate
MCM	Mine Counter Measure
PC	Patrol Craft
CNO	Computer Network Operations
CONUS	Continental United States
IP	Internet Protocol
MISO	Military Information Support Operations
EW	Electronic Warfare
IW	Information Warfare
EA	Electronic Attack
ES	Electronic Support
EP	Electronic Protection
EM	Electromagnetic
CND	Computer Network Defense
SEWIP	Surface Electronic Warfare Improvement Program

NROTC	Naval Reserve Officer Training Corps
C2W	Command and Control Warfare
MILDEC	Military Deception
OPSEC	Operational Security
GPS	Global Positioning System
RF	Radio Frequency
UAV	Unmanned Aerial Vehicle
OODA	Observe Orient Decide and Act
APPS	Afloat Print Production System
LRAD	Long Range Acoustical Device
SSES	Ship’s Signals exploitation Space
ACAT	Acquisition Category
LCC	Blue Ridge Class Command Ship
LPD	Amphibious Transport Dock
LSD	Landing Ship, Dock
HGHS	High Gain High Sense Receiver
ONR	Office of Naval Research
GCCS-M	Global Command and Control System-Maritime

ACKNOWLEDGMENTS

Thank you to my husband, Jeff, for being a sounding board for ideas, taking care of our home while I studied, and for putting up with the countless hours logged on the computer while researching and writing this thesis.

I would also like to thank Steve Iatrou for his guidance in the ways of information operations and for changing the way I think about information and its effects on human behavior and decision making.

Lastly, I would like to thank Capt Deidre McLay for her advice and support during the daunting task of completing a surface warfare-related thesis. I enjoyed our weekly chats to keep me on target.

Thank you for helping navigate the way back to my SWO roots!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Although the Navy's increased emphasis is on information dominance (ID) there is little to no documentation that matches Navy assets to ID rhetoric. Without guidance how will commanders understand how they may use ships to carry out the information dominance and information operations missions they may be tasked to accomplish? How does the Navy maximize the war-fighting effects associated with shipboard systems, through the information and physical domains, to optimize access of friendly forces to the information domain, while degrading or denying access to the enemy? These are the types of questions that need to be considered when developing a strategy for employing ships to achieve information dominance.

The Navy views information itself as a vital asset to mission accomplishment, but it does not clearly define how it will use its ships within the realm of information dominance and while conducting operations in cyberspace. U.S. Navy ships such as the Aegis guided missile cruisers (CG) and destroyers (DDG) provide highly mobile platforms capable of carrying out multiple missions within and in support of the realm of information dominance.

There is no consolidated go-to document that lists how planners can effectively use naval surface ships, such as a cruiser or destroyer, in information dominance and cyberspace operations. Doctrine may list how to conduct operations but it does not specifically list how to employ the multiple capabilities of individual platforms.

Capabilities lists that may be of use to planners would include non-kinetic fires capabilities and which platforms have the ability to provide measures of effectiveness once those capabilities are used. These measures of effectiveness could measure the correlation between the level of integration of non-kinetic fires within a mission, to support the effectiveness of kinetic fires, to the success of that mission. Lost in the discussion of the "what" of information dominance is the "how" to accomplish it; the "how" comes through the execution of information operations.

Information operations account for all aspects of military operations in the information domain. Information dominance may be viewed as the goal of information operations. Just as the Navy conducts air operations and anti-air warfare as measures to achieve air superiority, it learns how to conduct information operations in order to achieve information dominance. Information operations are what the Navy does to achieve a state or condition of information dominance. The mission of information operations in support of information dominance is to successfully conduct information operations and control the information domain (US Office of the Joint Chiefs of Staff, 2012). Ships are one tool that the Navy has to conduct information operations in support of information dominance.

The current configuration of surface naval vessels will be discussed; including the manner in which surface ships such as the Aegis guided missile cruiser (CG) and destroyer (DDG) fit into the modern era of naval information operations to achieve information dominance.

The advantage of using ships within an overall campaign or battle plan will be explored as well as what these platform's capabilities have to offer to IO planners.

To achieve this, an evaluation of past experiences and current technology will be used to recommend implementation of current surface ship information operations (IO) capabilities as well as an evaluation of information dominance and the domain of cyberspace, focusing on the areas of electronic warfare, cyber warfare, and military information support operations (MISO).

A. RESEARCH QUESTIONS

To what extent, if any, can current naval surface ships become an effective tool for achieving information dominance and for operating within the cyber domain?

In conducting this analysis, this thesis will address the following questions:

- How do Navy ships use the elements of information operations to achieve the Navy's mission of achieving and maintaining information dominance?
- What do surface combatants bring to this fight that cannot be executed remotely from CONUS, that is, as things become more and more Internet Protocol (IP) Centric.
- How do Navy surface combatants fit into Computer Network Operations (CNO)?
- What does the changing world of EW look like in a Task Force environment?
- How do we ensure that what information really matters gets to the decision makers regarding Information Dominance, so the question of "so what" is answered regarding capabilities?

B. DISCUSSION

> Information Dominance is the Navy’s initiative to maintain the Competitive Advantage in the Information Age.
>
> —ADM Gary Roughhead, CNO

The Chief of Naval Operations vision and guiding principles regarding information dominance is to pioneer, field and employ game-changing capabilities, ensuring information dominance over adversaries and decision superiority for commanders, operational forces and the nation as a whole. The first set of principles includes, but is not limited to:

- Utilizing every platform as a sensor
- Ensuring every sensor is networked
- One operator controlling multiple platforms
- An increasingly sea-based unmanned air systems capability
- A commonality in interfaces, data-links, and control systems
- Every shooter having the capability of using target data derived from any sensor (Dorsett, 2010).

These principles can be applied to Navy ships and the way they operate: Ships are a platform of sensors designed to network with other ships and forces, sharing targeting data as well as information for basic situational awareness. This information is provided through common/ compatible tactical data links. Ships are also organized into battle groups where each warfare area is centralized under warfare commanders.

Traditionally, the Navy has operated within a platform-centric view of warfare where emphases of effects and planning are based on individual independent platforms where the sensor, shooter, and decision maker were all from the same unit or platform (Dunn, Powell, Martin, Hamilton, & Pangle, 2004). In a platform-centric environment, ship captains would operate as autonomous units, not necessarily communicating with other units to complete their mission. With the drive to adapt the Navy's strategy to a more networked approach, the Navy's approach to information dominance includes initiative to move from platform-centric to information, or network-centric processes that would help create a fully integrated intelligence, command and control (C2), and cyber/networks capability. With the current configuration of modern warships providing satellite communications and common tactical data-link architecture, this networking of resources and information processing capabilities is what is necessary to be successful in a modern warfare environment. A fully integrated information operations capability, once fully realized, may prove to be the most valuable weapon against the adversaries of the United States (Dorsett, 2010).

The Navy has shown its commitment to fulfilling its goal of information dominance through:

- The establishment of the Information Dominance Corps (IDC) and manning that corps through recruitment and training programs designed to pull from current fleet assets/personnel
- The development of new personnel qualification standards (PQS) and the new Information Dominance Warfare Pin

- The establishment of cyber warfare centers at the USNA and NPS
- The establishment of an NROTC cyber scholarship program.

The most visible commitment to information dominance was the establishment of the new Tenth Fleet (C10F)/Fleet Cyber Command. The establishment of this new command has elevated information to a core naval war-fighting mode and capability set (Dorsett, 2010). This new core of information professionals needs to integrate with current navy units and establish training for the fleet as a whole regarding the power of information and information dominance.

This evaluation will suggest how surface assets, such as CGs, DDGs, and amphibious ships should be used as information operations assets. Suggestions will be made on how to incorporate and adapt current surface ship capabilities for use in the fast paced realm of information dominance. Navy information dominance strategy needs to incorporate the surface fleet and provide training to IO planners to ensure they understand how to effectively incorporate surface ships as tools within information operations.

C. BENEFIT OF THE STUDY

This study will provide individual ship commanders and crew, IO planners, as well as fleet leadership a better understanding of how information influences and is used to develop battle plans and when making command decisions. It will explore the way surface ships such as cruisers and destroyers are used as assets to help achieve the goal of information dominance.

The limitation of this study is that it will be limited to unclassified information and will not describe surface ship capabilities that are classified.

D. ROADMAP OF THESIS: A CHAPTER OUTLINE

This thesis is organized into six chapters: Chapter I provides an introduction to include areas of research, benefits of this study, and a roadmap to this paper. Chapter II provides a background of information operations and the concept of information dominance, globalization impacts, and electronic warfare.

Chapter III lists current configuration of U.S. surface ships for C4I/ISR and EW as well as an emphases on the specific systems involved. The AN/SLQ-32, AEGIS, LRAD, and future programs are included.

Chapter IV discusses information dominance, what ship capabilities help support information operations, and the vulnerabilities of an increased reliance on IP-based technology.

Chapter V is the conclusion of this thesis. It summarizes the study and provides suggestions for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. INTRODUCTION

The industrial age of the 1700–1900s has given way to the current information age. Leaders of modern militaries comment about a revolution in military affairs, where attacking information systems, as well as protecting one's own system(s), will play a substantial part in conflicts of the future (Poisel, 2002). From this is born military information operations (IO), previously referred to as command and control warfare (C2W), where protecting and attacking information and the systems, or system of systems, that process it, comes into play (Poisel, 2002). This way of understanding IO is outdated and focuses more on an impediment to achieving information dominance; it focuses on technology and our Navy's reliance on it with little emphasis on learning the nature of the information itself and its impact on human behavior. There needs to be a balance between the physical technology driven side and the information centric side of IO. Terms such as information-centric warfare and decision superiority have little meaning to ship commanders trying to complete IO missions without first understanding information's role in the decision making process.

B. WHAT IS *INFORMATION*

Information: "the communication or reception of knowledge or intelligence; knowledge obtained from investigation, study, or instruction" (Merriam-Webster, 2013).

Information Superiority: "*The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same* (Department of Defense, 2012)."

Information Environment: "*The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information* (US Office of the Joint Chiefs of Staff, 2012)."

Within the realm of information operations a commander's actions are based on a decision and that decision is based on information. Information is what ultimately drives behavior. Information is used to help explain reality, to help a ship's commander know, to the best extent possible, all possible events or scenarios that may take place, based on his current situation, and through how the current environment is perceived. The way a commander perceives his environment is affected by past life and professional experiences, by the accuracy of information gathering and processing capabilities, and by what is currently happening, i.e., the commander's momentary situation (Lippmann, 1943). The process of human decision making is what information operations is all about, regardless of the technology used to gather information or in the execution of information operations.

No one can ever truly understand, know, or comprehend everything that is occurring within one's current environment. At sea, a ship's commander is only truly aware of the immediate surroundings, like the status of visual contacts, weather, and sea state; the rest of its information environment is taken from links to other ships and information taken in by the ship’s sensors and is accepted to be true based on past experience. The best a commander can do is make an educated guess based on personal evaluation of the information at hand (see Figure 1). This perceived or pseudo-environment is the environment upon which a commander is basing decisions; the actions taken within this pseudo-environment will have effects in the real environment (Lippmann, 1943). A commander’s ability to assess the effect of his actions and whether they fit into his perception of reality is one way in which he can gauge how accurate the command’s information processing capabilities are. The closer the expected outcome from a decision/action is reflected in the actual outcome may be a way to measure the effectiveness of the information used to formulate that decision.

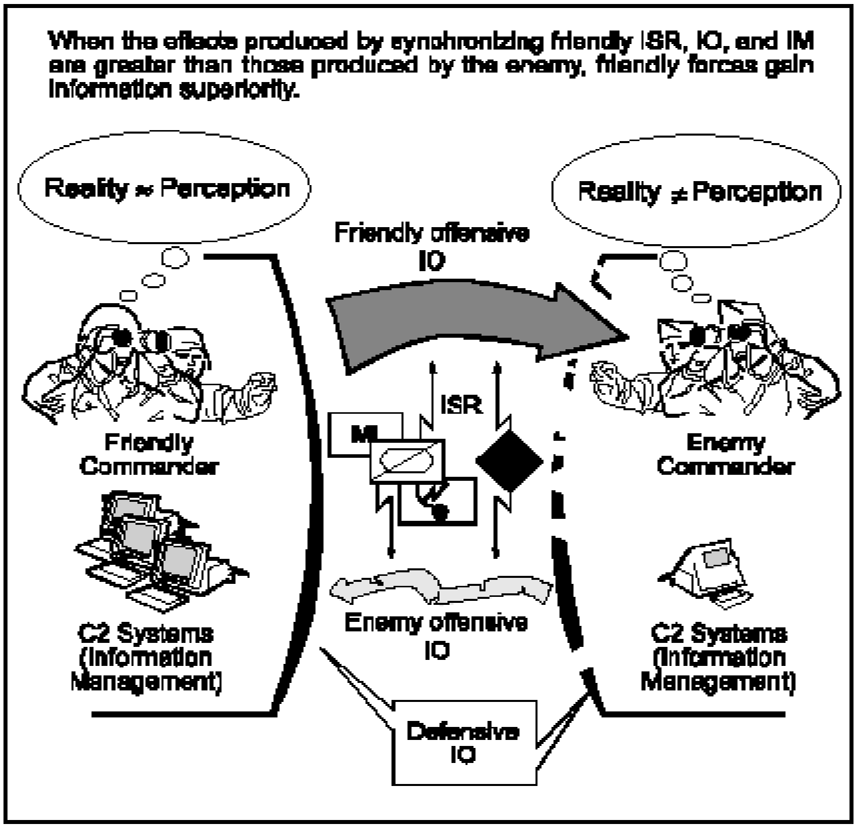
When the effects produced by synchronizing friendly ISR, IO, and IM are greater than those produced by the enemy, friendly forces gain information superiority.
Reality ≈ Perception
Reality ≠ Perception
Friendly offensive IO
ISR
MI
Friendly Commander
Enemy Commander
C2 Systems (Information Management)
Enemy offensive IO
C2 Systems (Information Management)
Defensive IO

Figure 1. Goals of information superiority (From U.S. Army FM 3-0 ch 11, 2013)

The Navy exists within an information environment that affects the cognitive, physical, and information dimensions (Figure 2) of the commanders that lead it. (US Office of the Joint Chiefs of Staff, 2012). Information permeates all aspects of operations through television, radio-communications, instructions from throughout the chain of command, and the Internet. The concept of information has an impact on every aspect of our everyday lives, and information can be the deciding factor of whether or not a commander is successful, or fails, at accomplishing his mission (Floridi, 2010). How commanders learn and make decisions is based on the information fed to them by their staff or through their own experiences.

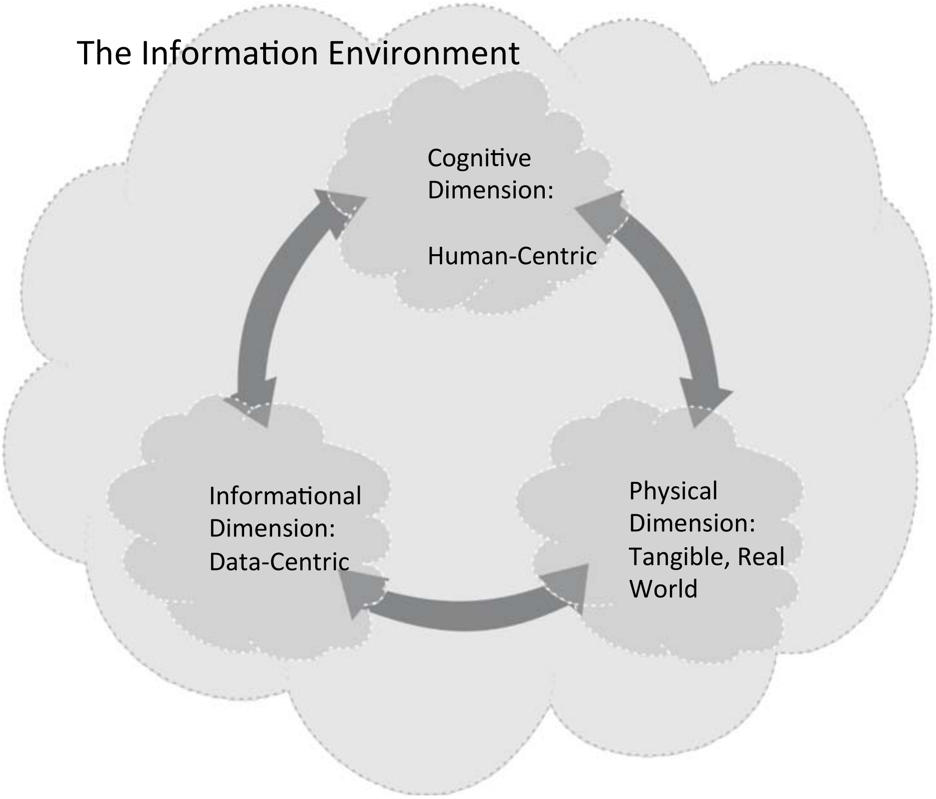

Figure 2. The information environment (From JP 3-13,2012)

Information operations, as applied in a military setting, is comprised of five pillars: (1) computer network operations (CNO), (2) Military information support operations (MISO) (formerly known as Psychological operations), (3) military deception (MILDEC), (4) operational security (OPSEC), and (5) electronic warfare (EW) collectively known as information related capabilities (IRCs). These pillars, in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own (US Office of the Joint Chiefs of Staff, 2012). These aspects of information operations may be applied to the capabilities and daily activities conducted in shipboard operations.

Computer network operations are comprised of computer network attack, computer network defense, and all other operations related to the enabling of computer network exploitation (U.S. Army War College, 2011). The use of computers to communicate to entities outside the physical boundaries of the ship, as well as onboard ships has increased the ability of sailors, and those outside of the Navy, to access information and to possibly disseminate information outside of the lifelines of the ship. This makes information more vulnerable, by creating another channel that may be exploited by the enemy, increasing the need to put into place measures to protect it and to prevent opportunities where information may be exploited.

In Joint Doctrine, Joint Publication 3-13.2, Military Information Support Operations (MISO) are defined as planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator’s objectives (US Office of the Joint Chiefs of Staff, 2011). Surface ships can support these operations by providing equipment to support pamphlet drops, the man power to help build schools during stability operations, and working with public affairs directorates to help boost strategic communications efforts to garner favorable sentiments toward the U.S. flag during ship port visits and community relations projects.

Deception involves actions that create the appearance of a situation that does not actually exist. It can be accomplished through the employment of decoy forces or radio and paper transmissions used to lead an adversary to false conclusions. An example of Military deception (MILDEC) operations during the first Gulf War was the movement of U.S. and coalition forces on the Saudi Arabia side of the Kuwait border that created the appearance of an attack against Saddam Hussein's forces in Kuwait in the incorrect region (Poisel, 2002). Deception can also be used to convince an enemy that forces are smaller or larger than they actually are or to mask their true identity. During World War II the allies' Navy was able to convince the Germans that the size of the allies' force was much larger than it was (Breuer, 1993).

"Loose Lips May Sink Ships" is a common phrase used to emphasize how important operational and information security are to shipboard operations. Operations security procedures are enacted onboard ships to help protect indications of upcoming operations. This can be through measures such as ensuring classified material is handled via proper methods and channels, and through taking care not to give away sensitive information through conversations and day-to-day interactions with others. The Navy stresses that OPSEC is every sailor's responsibility and with the increased availability of computers onboard Navy ships this responsibility becomes more important.

The largest area of information operations that is traditionally attributed to surface ships is Electronic Warfare (EW). Electronic warfare involves operations within the electromagnetic (EM) environment and is waged to secure and maintain the freedom of action in the electromagnetic spectrum. EW includes three major areas: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). The purpose of EW is to deny the enemy an advantage within the EM spectrum while ensuring friendly unimpeded access to the EM spectrum portion of the information environment (US Office of the Joint Chief's of Staff, 2007).

C. COMMAND AND CONTROL

Command and control (C2) is the exercise of authority and direction by a purposely-designated commander over assigned forces in the accomplishment of the mission (Coakley, 1992). In the Navy, C2 functions are performed through an arrangement of personnel, equipment such as ships and aircraft, communications (that may be visual, over radio, or through IP-based networks), and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission (Coakley, 1992). This definition treats C2 as a collection of command functions and those systems of people, procedures, and equipment that support command (Coakley, 1992). External communications and support systems facilitate the information exchange required to build and maintain an effective C2 system (Navy Warfare Development Command, 2011). Information and how it is relayed is the basis of any C2 system and this is reflected in the web-like nature of C2 networks (Coakley, 1992).

The terms command and control can be used as both verbs and nouns. As verbs, they describe the process of what a commander does, and as nouns, they name a system. They are the arrangement of people, equipment (hardware and software), and the procedures that help commanders do what they do (Coakley, 1992).

The procedures involved with a C2 system, like the actions that result from a commander’s decision cycle, have been derived from experience, common sense, the lessons of military history, and military theory. They constitute shared knowledge, the common thread that unites the minds of commanders from the top to the bottom of a chain of command. The procedures range from Service doctrines, which govern the use of weapons systems, to the principles of war, which guide commanders in their choices of strategies and tactics (Coakley, 1992).

As part of a C2 system, Navy Commanders first receive orders, a mission, or a senior commander’s intent regarding a situation. They then attempt to gather as much information as they can about his environment to better facilitate situational awareness and to help develop or drive the decision making process to fulfill their task at hand (Coakley, 1992). Onboard Navy ships a thorough understanding of C2 resources is vital to watch-standers, especially the tactical action officer (TAO), situational awareness and watch-standing capability (Navy Warfare Development Command, 2011).

An increasingly significant threat to effective command and control is warfare conducted in the cyber-domain. The use of IO tactics to disrupt the C2 loop, especially via the cyber-domain, can cause confusion regarding the authenticity of orders transmitted, and may give an adversary the ability to inject false information into the data-gathering process (Macke, 2013). Attacks can interrupt the connectivity between nodes and cause failure or delays of the C2 decision cycle. Understanding the vulnerabilities of C2 systems and ensuring that not all aspects of the decision chain are reliant on connections to the cyber-domain are two tasks vital to the success of information dominance (Macke, 2013). With C2 it is important not to put all of your eggs in one basket. Ensuring that C2 systems are capable of operating within and outside of a degraded or compromised cyber-domain is important to ensure reliable command and control.

D. GLOBALIZATION

The importance of a Navy rests on two pillars: its ability to affect events on land and its ability to control use of the sea, which includes the realm of commerce through seaborne trade. If the U.S. Navy wants to remain the dominant modern maritime force, it needs to recognize the impact globalization may have on these two pillars. Globalization as a phenomenon consists of substantial expansion of cross-border networks and flows; such flows may include the creation of global financial markets, expansion of democratic governance, or the increased ubiquity of the Internet and other forms of communications via modern information technology (Tangredi, 2002). Globalization illuminates the importance of evaluating the methods currently used to conduct information operations. Navy information professionals and planners need to ensure the approaches used when carrying out information operations take into consideration the effects globalization has on information and an adversary's capabilities.

A likely effect of economic globalization is a continuing increase in the capability and proliferation of high-speed information systems and remote sensors. A particular concern to naval forces is the increased availability of commercial satellite imagery, communications, and navigation systems. GPS allows for accurate attacks and navigation and space-based communications are more difficult to jam (Tangredi, 2002). The ability to detect via space-based systems may prove to be a vulnerability—could cause vulnerability of detection by space-based systems—but it is still unclear how capable adversary's abilities will be to use this against the U.S. Navy (Tangredi, 2002).

The world's oceans are sometimes called "the great common," open to all nations with the desire, access, and resources to master it. Oceans are the medium by which 90% (weight and volume) of world trade is transported and the medium by which the U.S. Navy has exerted its dominance (Tangredi, 2002). The increased reliance on modern technology requires the Navy to exert its dominance over the invisible cyber and information realm just as it does over the physical and visible maritime realm. The effects of globalization may require some collective self-searching: even though most communication links seem to be over the air or Internet, the surface Navy and surface warfare remains the most reliable on-station assets to support or relay those links (Tangredi, 2002).

E. ELECTRONIC WARFARE

The advent of the information age has brought about an almost universal reliance of society on wireless electronic communications. Even with the advent of software-defined radio, the reliance is still based on the RF spectrum. This reliance is shared by civilian businesses as well as the military. Cell phone systems are bringing these wireless communication systems to the mass public, but nowhere is this reliance on radio frequency (RF) technology more evident than in the military’s execution of command and control over its tactical forces (Poisel, 2004). Since use of RF communications is vital for tactical commanders to execute control over their forces, an adversary will have obvious interest in disrupting these communications, either through denial of use or through the interception of the information contained in them (Poisel, 2004). Electronic warfare is the name applied to actions taken to accomplish the intercept or denial of voice and data, including wireless, communications (US Office of the Joint Chief's of Staff, 2007). It is the need to prevent the enemy from disrupting our ability to freely and effectively use wireless communication channels that makes electronic warfare (EW) capabilities so important in the fight to achieve information dominance.

The core, supporting, and related information operations capabilities all directly or indirectly benefit from EW. Principle EW activities have been developed to exploit the opportunities and vulnerabilities that are inherent in the physics of RF technology and EM energy. EM activities include, but are not limited to: electrooptical-infrared and radio frequency countermeasures; EM compatibility and deception; EM hardening, interference, intrusion, and jamming; electronic masking, probing, reconnaissance, and intelligence; electronic security; emission control; and spectrum management (US Office of the Joint Chief's of Staff, 2007).

There are three major subdivisions within EW. They are Electronic Attack (EA), electronic Protection (EP), and Electronic Support (ES) and all three contribute to both offensive and defensive Information Operations capabilities (Naval War College, 2012). The outputs of all three areas of EW capabilities (EA, EP, and ES) impact the decisions of commander or tactical watch-standers. They rely on their ship's EW capability to provide the information necessary to evade detection or attack by an adversary or to interrupt and degrade their adversary's capabilities.

Electronic attack is concerned with denying an adversary commander or unit access to the use of the electronic spectrum to effectively command and control their forces (US Office of the Joint Chief's of Staff, 2007). EA involves actions taken to attack with the intent of degrading, neutralizing, or destroying an enemy's combat capability. Electronic protection involves the ability to guarantee the use of the electromagnetic spectrum for command and control of friendly forces. EP actions may include self-protection jamming and emission control to minimize the effects of EW, either friendly or enemy, on friendly forces ability to use the EM spectrum. Electronic Support contributes to a commander's ability to accurately estimate a situation in the operational area by detecting, identifying, and locating sources of intentional or unintentional radiated electromagnetic energy to contribute to immediate threat recognition (Naval War College, 2012).

Electronic Warfare is the most widely used element of information operations at the tactical level. EW tradeoffs are the relative benefits of EA versus ES for specific missions/operations. ES tells a commander a great deal about the location of an adversary and what they can see or jam, and when deciding to conduct an EA operation a commander must realize and plan for the ES information they may be giving up (Naval War College, 2012).

III. CONFIGURATION OF SURFACE SHIPS FOR IO

A. INTRODUCTION

When using a naval surface ship for information operations, what unique capabilities are available because of that ship's presence? All surface ships' assets capabilities are tied to the information domain, by the fact that they are involved in the collection, delivery, analysis, or modification of information, but not all are tied to the domain of cyberspace. A ship could be used as a persistent local presence for jamming, but its effectiveness depends on the ability for it to remain undetected and to provide enough signal strength to reach and disrupt the targeted signals. Another use than jamming or anti-jamming may be using the ship as a C2 platform to orchestrate and direct the actions of other more maneuverable air and surface assets- like small UAVs. Surface ship capabilities may also include non-kinetic fires and the ability to provide the integration of information to increase the effectiveness of kinetic fires.

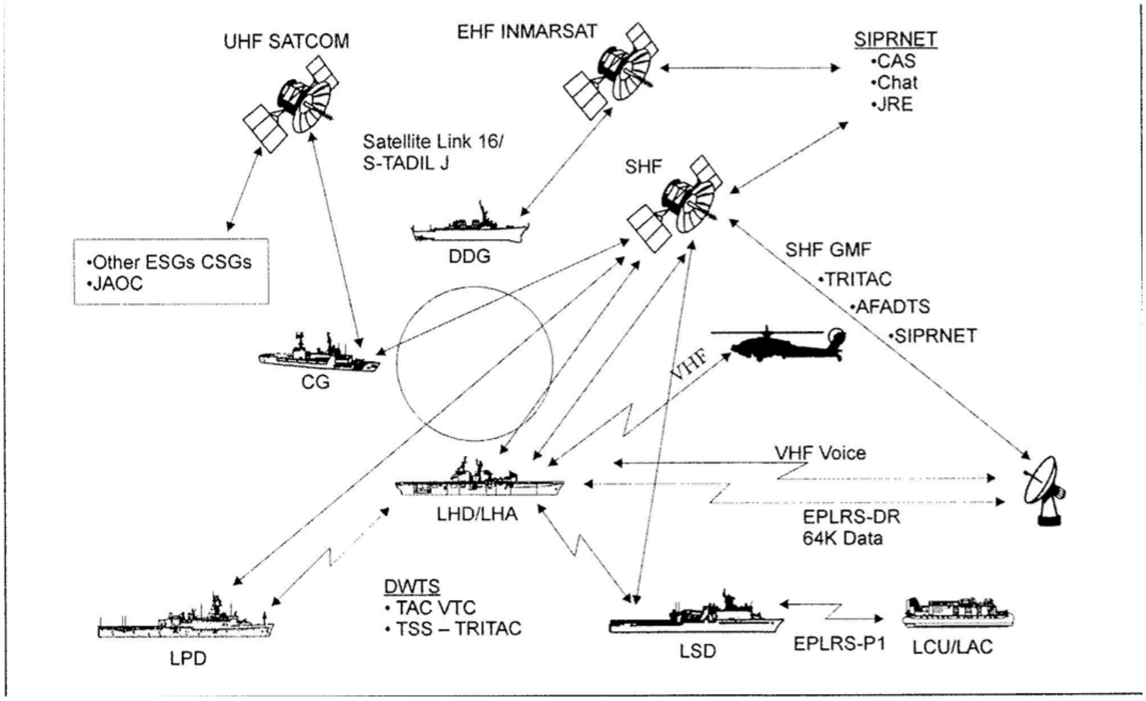

Figure 3. Example of shipboard satellite communications (From Surface Ship Operations, 2012)

The proliferation of advanced military systems—such as intelligence, surveillance, reconnaissance sensors, as well as ballistic and cruise missiles parallels the post-Second Gulf War operational concept on how to defeat U.S. forces, known as anti-access, or area denial strategy. Instead of fighting U.S. naval forces on a regional battle space, future adversaries may attempt to prevent U.S. or coalition forces from reaching the battle space or they may attempt to engage first through the denial of information or through cyberspace. The goal of an anti-access strategy is to convince U.S., and coalition partners, that the cost of penetration is simply too high (Tangredi, 2002). If the Navy, including surface ship commanders, is able to maintain dominance of the cyberspace and information domains it may be able to negate the effects of an adversary’s attempt at an anti-access strategy.

When planning how to conduct an information operations mission to achieve information dominance a commander needs to determine what information he needs, what capabilities he has to achieve his mission’s goals, his information processing needs, and how he will measure the effectiveness of his actions. Table 1 lists some of the major capabilities of Navy surface platforms that help commanders make decisions through situational awareness and providing information of the battle-space in a way that may give his OODA loop/decision cycle an advantage over an adversaries’.

B. CURRENT U.S. NAVAL SURFACE COMBATANTS IO CAPABILITIES

1. Aegis

Aegis is a computer-based networked command and decision combat system capable of simultaneous operations against multi-mission threats. The Aegis system was designed as a total detect-to-engage weapon system. At the heart of Aegis is the AN/SPY-1 series radar system, an advanced, automatic detect and track, multi-function phased-array radar. This high-powered radar performs search, track and missile guidance functions simultaneously with a track capacity of more than 100 targets. Aegis was designed to help warfighters compensate for the decrease in time available to make a decision and act during hostilities; it helps to speed up a commander’s OODA loop and decision cycle (Naval Sea Systems Command, 2012).

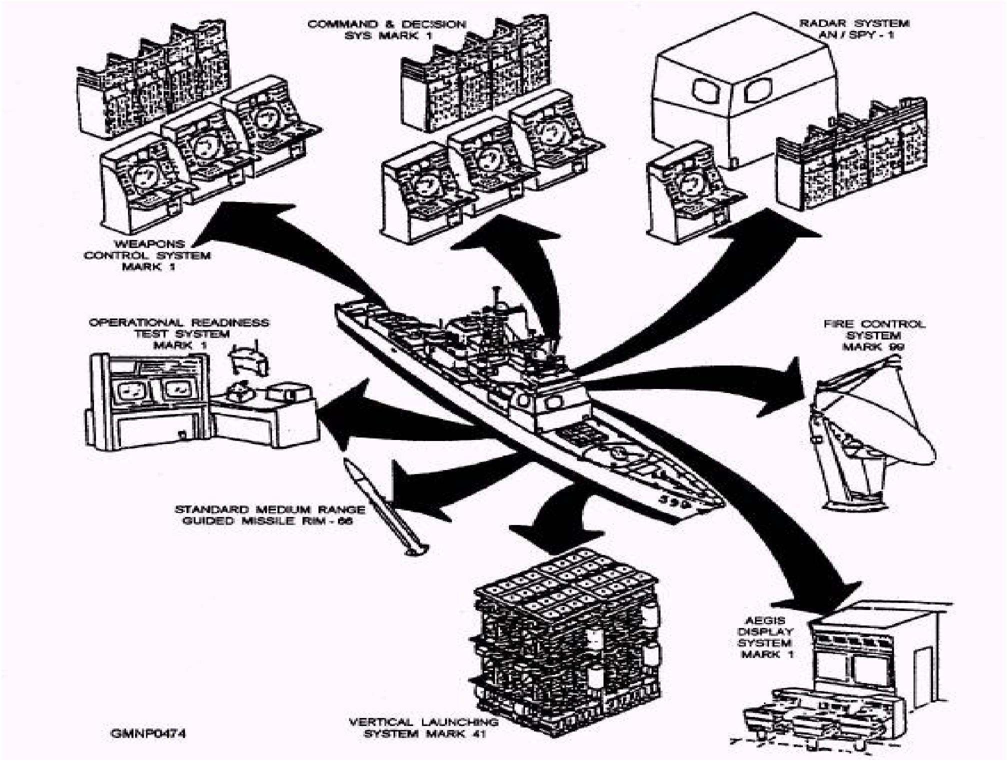

Figure 4. AEGIS weapon system Mk 7 major elements, (From Naval Sea Systems Command, 2012)

2. AN/SLQ-32

With the capability of adversary platforms to carry and launch multiple anti-ship cruise missiles (ASCMs) the need arose for an Electronic Warfare system aboard surface ships to meet this threat and the system developed was the AN/SLQ-32(V) whose external hardware can be seen attached to a U.S. warship in Figure 5 (Lewis, Elbourn, Schermerhorn, & Machleit, 1980).

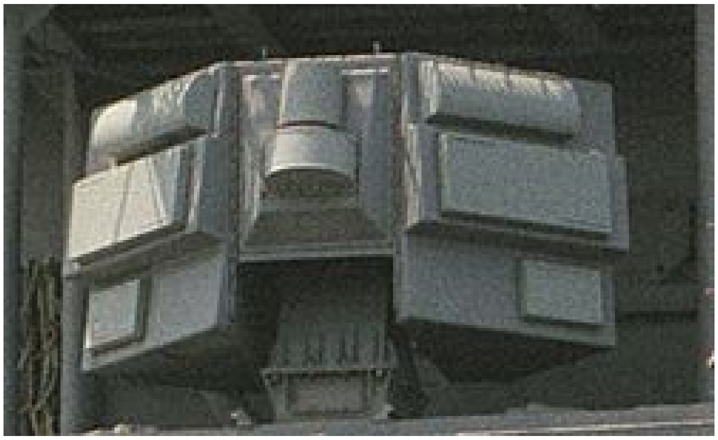

Figure 5. AN/SLQ-32 antenna (From Military Analysis Network, 1999)

The primary mission of the AN/SLQ-32 is to defend own ship against the ASCM threat. To accomplish this, the AN/SLQ-32 provides detection, identification, and bearing of radar guided ASCMs and their associated threat platforms. The AN/SLQ-32 operator reads the information provided by the AN/SLQ-32 on a screen window display like the one pictured in Figure 6. The active electronic counter measures (AECM) subsystem of the SLQ-32 uses jamming, a form of electronic attack, and/or deception techniques, which alter specific or generic ASCM trajectories, to disrupt the targeting information an adversary requires for a missile attack (Lewis, Elbourn, Schermerhorn, & Machleit, 1980).

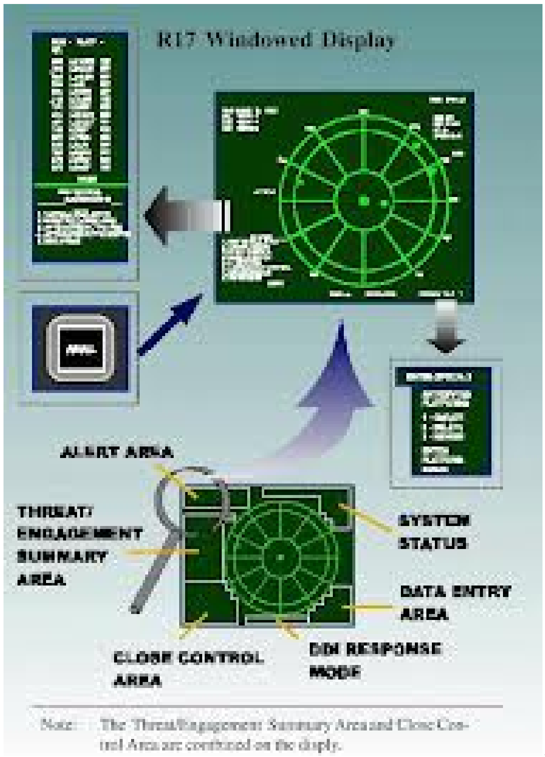
R17 Windowed Display
ALERT AREA
THREAT/ ENGAGEMENT SUMMARY AREA
SYSTEM STATUS
DATA ENTRY AREA
CLOSE CONTROL AREA
DDI RESPONSE MODE
Note: The Threat/Engagement Summary Area and Close Control Area are combined on the disply.

Figure 6. View of the display window of an AN/SLQ -32 (From Military Analysis Network, 1999)

3. Long Range Acoustical Device (LRAD)

Commanders have many long-range over the horizon sensors to help with their ability to acquire information, to affect enemy sensors, to help improve overall situational awareness, and to aid in decision-making. The Long Range Acoustic Device (LRAD) gives a ship’s commander the ability to affect the immediate area surrounding their unit in a non-kinetic way through the direction the LRAD is focused (Figure 7). LRAD is a portable device that provides clear and intelligible voice communications within 500 meters of its placement (see Figure 8). The audio interface of a LRAD allows its operators to relay recordings to its target audience in whichever language may be required. Missions supported by LRAD include:

- Water-side force protection
- Anti-piracy
- Visit board search and seizure (VBSS)
- MISO/ psychological operations (American Technology Corporation, 2004).

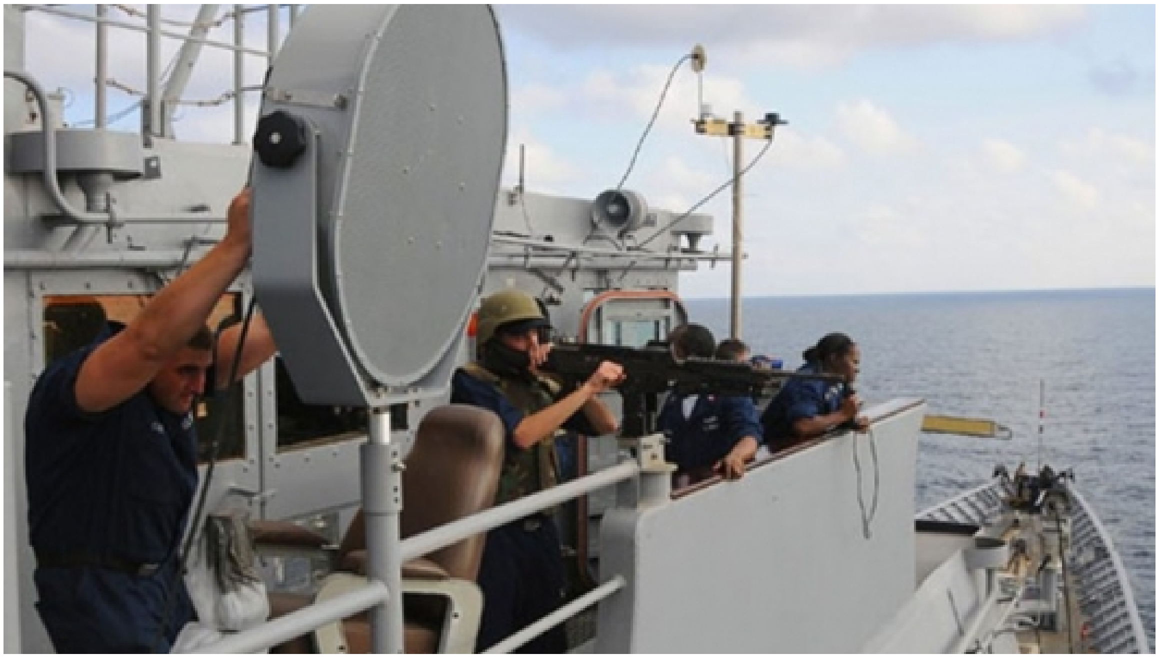

Figure 7. An example of LRAD operated onboard a naval vessel (From American Technology Corporation, 2004)

LRAD lets pirates or aggressors know that the targeted vessel is aware of them, and helps defenders determine intent in deciding when to escalate force-protection measures (Lundquist, 2010). LRAD functionality can also be used as a tool in a commander’s non-lethal Electronic Attack capabilities by its ability to produce large amounts of audible energy as seen in Figure 8 (American Technology Corporation, 2004).

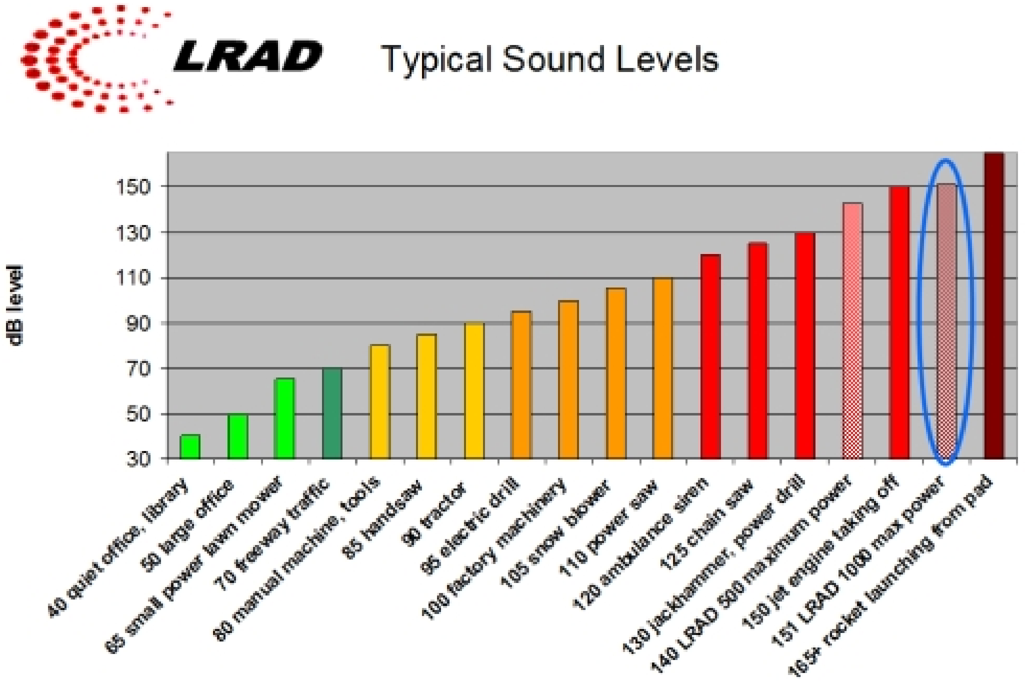

Figure 8. How LRAD compares to other sound producing devices (From American Technology Corporation, 2004)

4. Data LINKS/: GCCS-M, Link-11, and Link-16, CEC

One of the largest contributions a surface ship provides to information operations is its ability to provide and maintain the common operating picture (COP). The COP is enhanced with information gathered by information systems such as radars and other sensors and then organized and distributed using systems such as GCCS-M, Link-11, and Link-16 (Navy Warfare Development Command, 2011). Figure 9 depicts what the common operating picture may look like involving a surface Navy combatant that is providing information to forces on the ground.

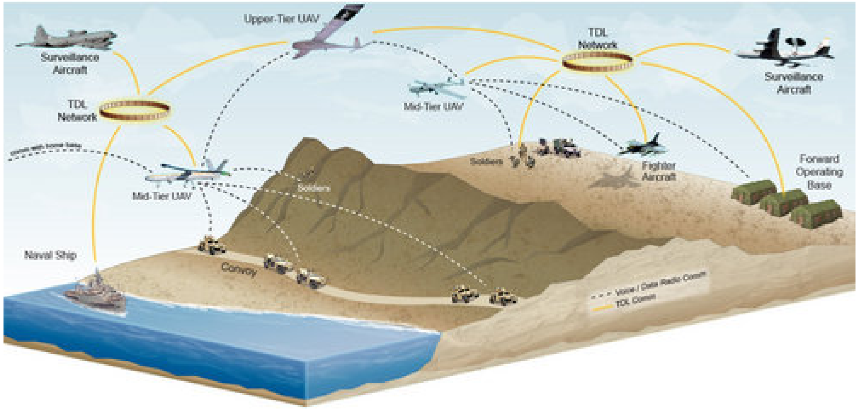

Figure 9. An example of a surface ship aerial COP via a TDL network (From Ultra Electronica, 2011)

Global Command and Control System- Maritime (GCCS-M) operates in a variety of environments in support of joint, coalition, and allied forces. It provides a single integrated and scalable C4I system that supplies information to aid Navy commanders, Tactical Action officers, and watch-standers when making tactical decisions. GCCS-M displays, at a near real-time capacity, the location of air, sea, and land units anywhere in the world and identifies them as friendly, enemy, or neutral units (Navy Warfare Development Command, 2011). Figure 10 shows how the different components of the GCCS-M system are organized and how information flows to and from functional components and the units that provide inputs and outputs to the common operating picture.

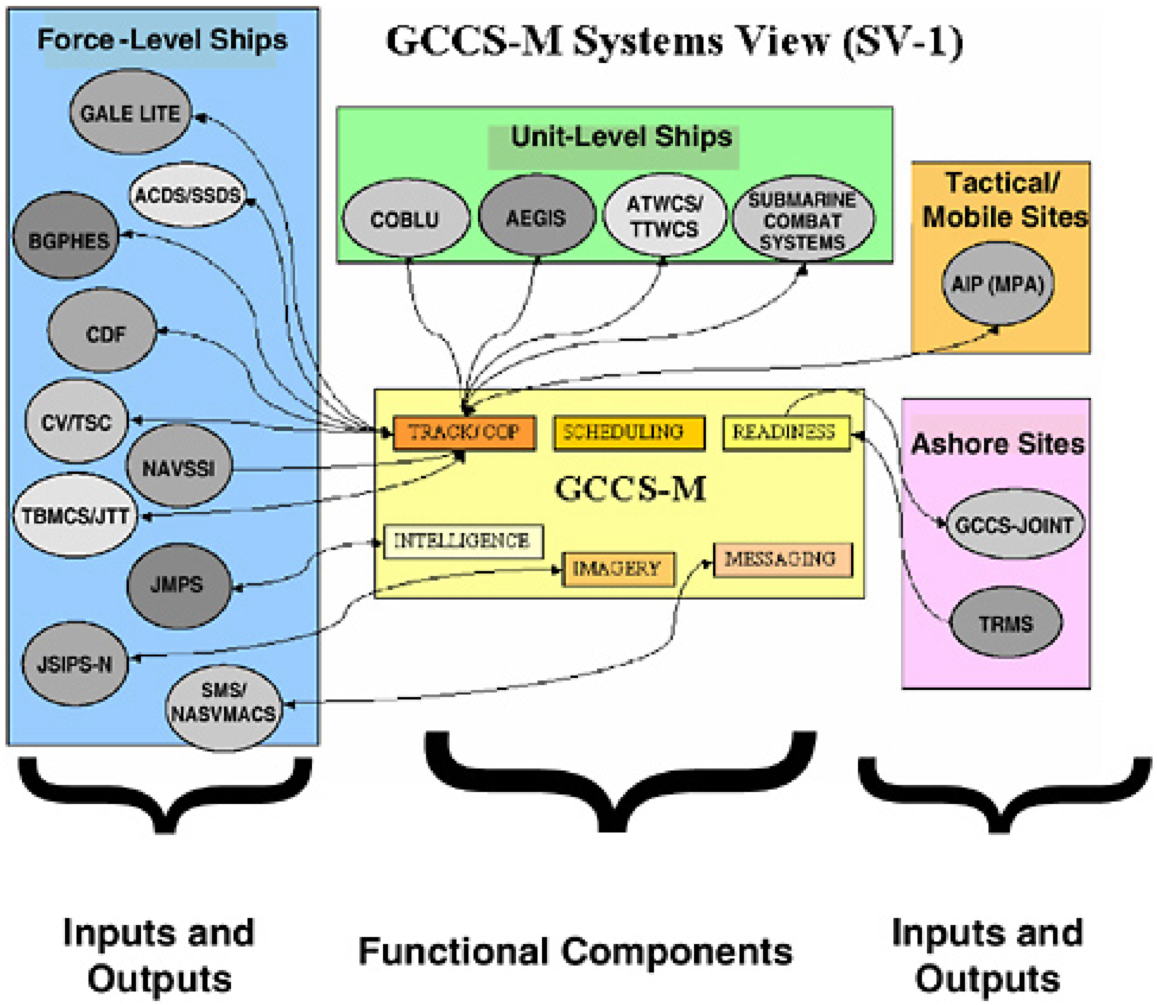

Figure 10. Global command and control system-maritime (GCCS-M) systems view, (From National Academies Press, 2013)

Tactical data link, such as Link 11, Link 16, and Cooperative Engagement Capability (CEC), interfaces provide a continuous exchange of information regarding friendly, hostile, and unidentified space, air, land, and subsurface tracks. They can provide the weapons status of friendly units as well as give their users to digitally transmit commands and requests to other commanders and units (Navy Warfare Development Command, 2011). Tactical data links provide a shared pool of information that can aid in shortening a commander’s decision cycle and situational awareness, but they can also be susceptible to jamming and not all forms of tactical data links are universal amongst friendly or coalition forces (Navy Warfare Development Command, 2011).

A commander can use the data gathered by GCCS-M in concert with data from other sources, such as Link-16, to construct relevant tactical pictures using maps, map overlays, imagery, oceanographic, or meteorological data. It provides a fusion plot of all tactical information relevant to the AOR. Supplied with information from GCCS-M and Link inputs, Navy commanders can review and evaluate the tactical situation, determine and plan actions and operations, direct forces, synchronize tactical operations, and integrate the maneuver of forces with firepower (Navy Warfare Development Command, 2011).

5. Privateer

Privateer is an EW support system found onboard Cyclone Class Patrol Coastal ships (PC). This support system helps extend the ability of commanders’ onboard PCs to contribute to the COP. It provides information to a commander to help make more informed decisions. It is comprised of two sub-systems capable of radar detection, identification, and location. Other capabilities of the Privateer system include:

- System RF input management
- General signal/spectrum search
- Director search for specified signals in specific portions of the signal spectrum

Applications that allow tactical cryptologic support operators to type, record, and playback selected extracts of communications in order to support threat Indications and warnings (I&W) analysis (Navy Warfare Development Comand, 2007).

6. Ship’s Signal Exploitation Space

The Ship’s Signal Exploitation Space (SSES) provides indications and warning support to tactical watch standers and strike group planners. SSES can provide real-time reporting and dissemination of time-sensitive information to national and tactical-level decision makers throughout the region, fleet, and globe (USS George Washinton Public Affairs, 2012).

7. Future Programs:

a. SEWIP

Goal 4 of the Navy Strategy for Achieving Information Dominance involves the continued development and research of systems to achieve integrated kinetic and non-kinetic fires. This goal states:

> To multiply war-fighting effects, the Navy will integrate kinetic and non-kinetic fires. To this end, the Navy will expand and strengthen its operations within cyberspace and the electromagnetic spectrum. To dominate in these areas, the Navy will further develop its cyber workforce, bolster related research and development, and refine its governance, policy, and TTP. Specifically, we must improve our active network defense and improve our cyber offensive capability. Likewise, the Navy must continue to advance its EW capabilities in order to disrupt

> adversary surveillance, targeting, and C2, and effectively counter anti-ship cruise missiles and ballistic missiles alike. (Department of the Navy, 2012)

In military operations, once a new weapon is developed another will be invented to counteract the first one. This is no different when it comes to EW, ISR, and C4I systems. Detailed information on hostile radar and other information related systems is usually unavailable making it near to impossible to design an intercept receiver as effective as the original system or radar receiver (Tsui, 2005). This makes the U.S. Navy's continued research and development into future programs and system improvement programs important if it is to keep ahead of our adversaries' capabilities.

In an era that features more and more supersonic ship-killing missiles, with better radars and advanced electronics, SLQ-32's fundamental electronic hardware architecture needs to be updated, and to accomplish this the Navy has initiated the Surface Electronic Warfare Improvement Program (SEWIP) (Defense Industry Daily, 2011). SEWIP is an ACAT II program designed to improve upon the current capabilities of the AN/SLQ-32 system and has been designed to release these improvements through block increments (Naval Sea Systems Command, 2012).

Block Design: SEWIP is an evolutionary development block upgrade program for the AN/SLQ-32 EW system currently installed on aircraft carrier and surface and amphibious warships (CVN, CG, DDG, FFG, LSD, LPD, LHA, LHD, and LCC) in the U.S. Navy. In early 2012, a total fleet-wide population of 150 systems was in operation. The SEWIP program is made up of four block upgrades:

Block 1 provided enhanced Electronic Warfare (EW) capabilities to existing and new ship combat systems to improve anti-ship missile defense, counter targeting and counter surveillance capabilities. Block 1 is focused on processor enhancement, improvements in the human machine interface of the AN/SLQ-32, Block 1A, and added a Specific Emitter Identification (SEI) receiver, Blocks 1B1 and 1B2, and High Gain High Sense receiver (HGHS), Block 1B3. The SEI and HGHS capability provides improved battlefield situational awareness (Naval Sea Systems Command, 2012).

Block 2 will provide an upgraded antenna, receiver and combat system interface for the AN/SLQ-32 system. Upgrades are necessary in order to keep pace with current threats and improve detection and accuracy capabilities of the AN/SLQ-32 (Naval Sea Systems Command, 2012).

SEWIP Block 3 focuses on Electronic Attack (EA) capability improvements required for the AN/SLQ-32(V) system. SEWIP Block 3 will provide a common EA capability to all surface combatants that have been outfitted with the active variant of the AN/SLQ-32, as well as CVN-78 and CVN-79 new-construction platforms. This Acquisition will leverage technology developed under the Office of Naval Research’s (ONR) Integrated Topside Science and Technology effort (Naval Sea Systems Command, 2012).

Block 4 will provide upgraded electro-optic and infrared capabilities to the AN/SLQ-32 system (Naval Sea Systems Command, 2012).

SEWIP was established as an ACAT II program in 2002 after cancellation of Advanced Integrated Electronic Warfare System (AIEWS). Development of SEWIP Block 1A, 1B1 and 1B2 are complete with upgrades in full rate production and Fleet-wide installations are in-progress. Development of SEWIP 1B3 is almost complete. The SEWIP Block 2 contract was awarded September 2009 and development is in progress. As of 24 October 2012, the SEWIP Block 3 program was still being established as the newest program/system able to support surface ships needs protect themselves from missile and other surface threats (Naval Sea Systems Command, 2012).

b. MQ-8B/C Fire Scout

Embarked Unmanned Aerial Vehicles (UAVs) are one way a surface ship can extend its information gathering and dissemination capabilities beyond the sensors hardwired into the ship. The Northrop Grumman Corp MQ-8 Fire Scout is a rotary-craft UAV designed to be deployed on FFGs, littoral combat ships, and other surface combatants, and the UAV's mission capabilities cover:

- Reconnaissance, ISR
- Situational awareness, including a night vision capability
- Anti-piracy
- Search and rescue
- Precision targeting (SUAS News Staff, 2012).

Payloads designed for the Fire Scout can include active and passive electronic warfare and electronic countermeasures equipment with an approximate eight hour on station capability and a more than 100-mile range; jamming, communications relay, and satellite communications are also possible (Walsh, 2012).

The MQ-8B Fire Scout has the ability to autonomously take off and land on any aviation-capable warship (figure 11) (Northrop Grumman, 2013). This UAV has been successfully tested onboard the frigate USS HALYBURTON were it completed a seven-month deployment alongside manned MH-60 Seahawks. During this deployment the Fire Scout demonstrated its ability to undertake missions involving anti-piracy and ISR (Donald, 2011). Having a UAV asset like the MQ-8B Fire Scout gives a ship's captain the ability to explore missions of longer duration or that are considered too dangerous for a manned helicopter or boat.

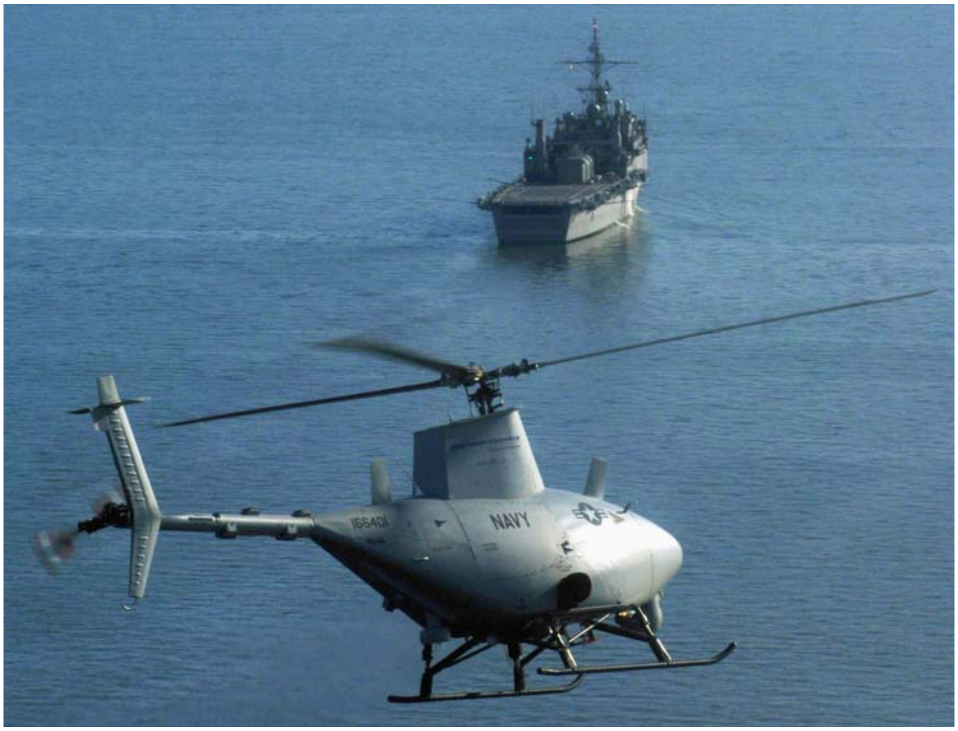

Figure 11. A Fire Scout prepares for the first autonomous landing aboard the USS ***Nashville*** (LPD 13) during sea trials in 2006 (From U.S. Navy, 2006).

In 2011, the Fire Scout successfully demonstrated the ability to send sensor data to the cockpit display of a MH-60 helicopter in addition to home ship displays. Fire Scout compliments the Navy's manned helicopters, which are vital ISR and ASW assets, by effectively expanding the range and area of ship-based intelligence gathering operations (Northrop Grumman, 2011). As development progresses with the Fire Scout program more ships may get the opportunity to test what a tactical unmanned aircraft offers to their common operating picture and decision making capabilities.

Table 1. Surface ship IO capabilities by platform

	CVN	CG	DDG	FFG	PC	MCM	LCS	LHA	LHD	LSD	LPD
GCCS-M	X	X	X	X	X		X		X	X	X
LINK-11	X	X	X	X				X	X		
LINK-16	X	X	X				X	X	X		
LRAD	X	X	X	X	X	X	X	X	X	X	X
AN/SLQ-32	X	X	X	X				X	X	X	X
SSES	X	X	X					X	X		
AEGIS		X	X								
Privateer				X							
SEWIP (Planned)	X	X	X	X				X	X	X	X
Fire Scout (Planned)	X	X	X	X			X	X	X	X	X

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SURFACE SHIPS IN THE INFORMATION DOMAIN

A. INTRODUCTION

> Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to space and cyberspace.
>
> —Secretary of Defense Leon E. Panetta

As a result of recent cyber activity, including Stuxnet and Flame, many countries are preparing for cyber warfare (Stillions, 2012). The U.S. Navy has formed U.S. Tenth Fleet and Fleet Cyber Command to provide guidance and to show how dedicated the Navy is to ensuring dominance in the cyberspace domain. The Mission of U.S. Fleet Cyber Command:

> The mission of Fleet Cyber Command is to serve as central operational authority for networks, cryptologic/signals intelligence, information operations, cyber, electronic warfare, and space capabilities in support of forces afloat and ashore; to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to execute cyber missions as directed; to direct, operate, maintain, secure, and defend the Navy's portion of the Global Information Grid; to deliver integrated cyber, information operations, cryptologic, and space capabilities; to deliver a global Navy cyber common operational picture; to develop, coordinate, assess, and prioritize Navy cyber, cryptologic/signals intelligence, space, information operations, and electronic warfare requirements; to assess Navy cyber readiness; to manage man, train, and equip functions associated

> with Navy Component Commander and Service Cryptologic Commander responsibilities; and to exercise administrative and operational control of assigned forces. (U.S. Fleet Cyber Command/U.S. Tenth Fleet, 2012)

Through this mission statement U.S. Fleet Cyber Command has developed its vision to conduct full spectrum operations in and through cyberspace ensuring Navy and joint/coalition freedom of action while denying the same to our adversaries. The Navy intends to achieve this end through Global situational awareness and command and control, operational requirements generation, work force development, and partnerships with the intelligence community, industry, and academia (U.S. Fleet Cyber Command/U.S. Tenth Fleet, 2012).

The mission of Tenth Fleet is to serve as the Numbered Fleet for Fleet Cyber Command and exercise operational control of assigned Naval forces; to coordinate with other naval, coalition and Joint Task Forces to execute the full three spectrums of electronic warfare, information operations and signal intelligence capabilities and missions across the cyberspace, electromagnetic and space domains (U.S. Fleet Cyber Command/U.S. Tenth Fleet, 2012).

Surface ships are able to support this mission through electronic warfare and information gathering and dissemination capabilities. Through military deception, information can be disseminated to influence adversaries causing them to believe in an information environment that does not reflect reality and causes them to act in a way beneficial to the U.S. and its allies.

Tenth Fleet’s mission to ensure freedom of action for the U.S. and her allies within the cyber domain can be compromised if ship commanders do not ensure their commands understand how their day to day activities affect the cyber domain. Surface warfare officers and enlisted sailors need to understand how personal connections over computer systems as well as the connectivity of the systems they operate in carrying out their duties may be connected to and affect security of operations in the cyber domain.

B. IP-BASED ENVIRONMENT

Modern ships exist and function in an Internet Protocol-based environment. The legacy model of voice or Morse code transmission via station-to-station has been replaced. Internet protocol or IP is the primary protocol that established the Internet. It is the principal communication protocol used for relaying packets of information across networks, called datagrams, as well as across network boundaries (Gehrke, 2012). IP defines an addressing system that functions to identify the hosts of the information as well as provides a location of that information, see Figure 11. Internet Protocol is vulnerable to attack and all Navy networks must be protected from adversaries who are rapidly gaining knowledge of IP weaknesses and exploits (Gehrke, 2012). Even with the proposed shift to the most current version of Internet protocol, IPv6, which is believed to be more secure, DoD IP-based systems and networks will still be vulnerable to Man-in-the-middle attacks, unauthorized access, as well as attacks on the physical/data-link layers of a system (Gehrke, 2012).

Ship’s data, through systems such as Global Command and Control System—Maritime (GCCS-M) and tactical data links, is exchanged via external communications channels, IP-based local area networks, and direct interfaces with other systems and networks (Navy Warfare Development Command, 2011). These systems are vital to a naval commander’s ability to make effective decisions. They are examples why a ship’s ability to conduct successful computer network operations (CNO) and EP measures is vital to mission success; failing to ensure access to required information via such systems would greatly hinder decision-making.

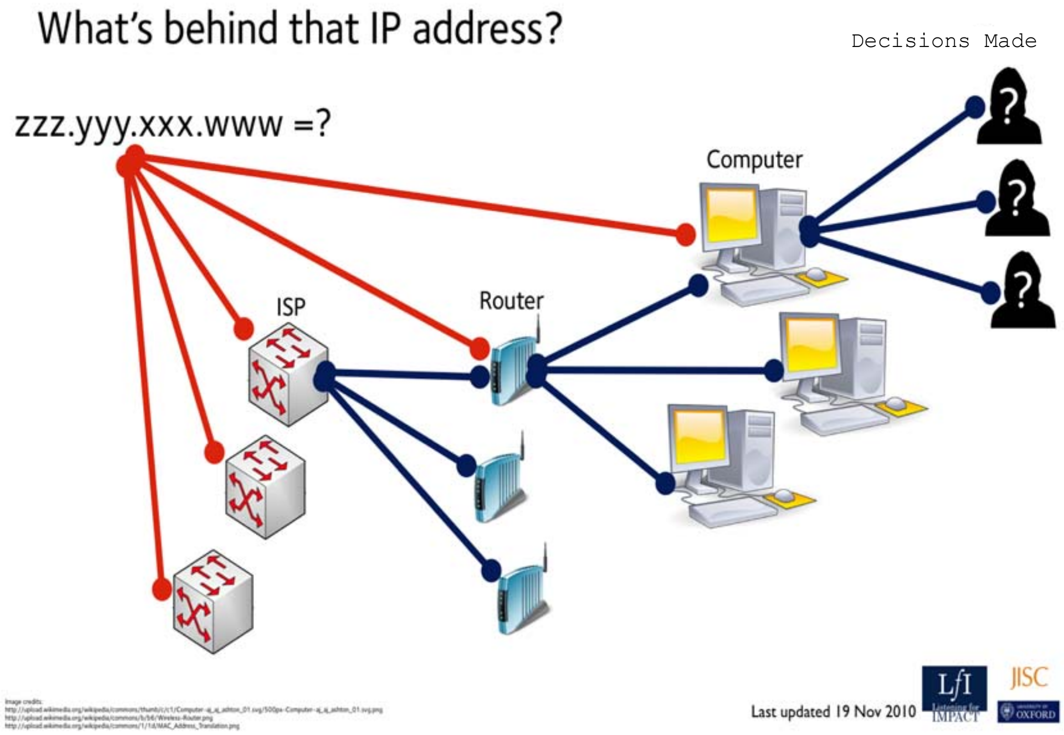
What’s behind that IP address?
Decisions Made
zzz.yyy.xxx.www =?
Computer
ISP
Router
?
?
?
Image credits:
http://upload.wikimedia.org/wikipedia/commons/thumb/c/c1/Computer-aj_aj_ashton_01.svg/500px-Computer-aj_aj_ashton_01.svg.png
http://upload.wikimedia.org/wikipedia/commons/b/b6/Wireless-Router.png
http://upload.wikimedia.org/wikipedia/commons/1/1d/MAC_Address_Translation.png
Last updated 19 Nov 2010
LfI Listening for IMPACT
JISC
UNIVERSITY OF OXFORD

Figure 12. What does an IP address lead to (After Oxford, 2010)?

C. WHAT DO SHIPS BRING TO THE FIGHT?

Ships may not provide anything more to information operations or the fight to dominate cyberspace than intensified protections of their own systems and those systems to which they are connected, including embarked UAS platforms like the Fire Scout that expand the reach of ships sensors. However, protecting own ship’s systems, connectivity, and information operations capabilities is an essential mission of a ship commander and requires focused effort and attention. The commander needs to understand this, but also needs to understand that the information gathering, dissemination, EW, and MISO capabilities of a ship are also vital information operations tools in the overall quest for information dominance by the force as a whole.

The mission of the U.S. Navy is to maintain, train, and equip combat ready naval forces capable of winning wars, deterring aggression and maintaining freedom of the seas (Department of The Navy, 2013). To fulfill this mission, an individual ship may serve in a direct or indirect role in support of achieving and maintaining information dominance. The capabilities of surface ships lend them to be information gathering platforms, electronic warfare platforms, and command and control platforms based on their tactical data link and communications capabilities.

The surface fleet provides a distributed, far field of sensors that can be netted together to fill gaps and holes in the world-wide intelligence picture; ships are persistent on station and have the acreage that other units do not, their sheer tonnage and available space can be used in ways and with payloads smaller assets are unable to accommodate (K. Eyer, personal communication, December 12, 2012). To share the results of information gathering, ships must remain securely connected to the information grid.

1. Kinetic and Non-kinetic Fires

The increased reliance of modern technology requires the Navy to exert its dominance over the invisible cyber and information realm just as it does over the physical and visible maritime realm. The popular slogan “putting warheads on foreheads” epitomizes the Navy culture of focusing on conducting kinetic fires, but this may not be the most efficient, effective, or appropriate way to engage adversaries in future conflicts. Surface ships most useful non-kinetic capability is its ability to conduct electronic warfare, and this contribution should be emphasized and exercised frequently.

Non-kinetic energy (NKE) weapons are weapons that seek to achieve their purpose other than through the threat or application of force to physical objects such as buildings, weapons systems, or the human body (Casey-Maslen, 2010). A non EW example of a non-kinetic method for controlling a situation would be the use of LRAD during anti-piracy operations. The effects of the LRAD may discourage the pirates from their target without the ship that is defending themselves from them having to fire even warning shots.

Non-kinetic fires enhance the ability to employ kinetic fires by removing the enemy’s ability to conceal himself through the use of information operations

(McConnell, 2005). Through military deception or jamming a Navy Commander can degrade an adversary’s ability to effectively engage and attack without physically destroying his capabilities. He or she can use deception to inject information into the information-environment to affect an opponent’s decision making capability. If a commander believes that a data link network has been compromised by an opponent a possible deception may be to add false contacts or resources into the common operating picture or mask how his own forces are displayed. UAS platforms could aid in this deception by mimicking a high value target. The cost of an enemy shooting down an unmanned target is much less than that of a manned aircraft. If an opponent is led to believe a target is in a false location he or she may waste their resources on that false target leaving the real target unharmed.

The Navy’s information dominance vision is to provide assured maritime command and control and superior battle space awareness to enable sustained, integrated fires across the full spectrum of modern maritime warfare (Department of the Navy, 2012). To achieve this vision the Navy strategy is to integrate kinetic and non-kinetic courses of action to accomplish objectives. Through the use of UAVs, tactical data links, and electronic support ships are able to maintain a robust common operating picture for use by the C2 construct. To protect the validity of the information the COP presents to decision makers and to reduce vulnerability to adversary’s sensors ships are able to conduct electronic protection and CNO directed at closing gaps that may be exploited in system software and IP connections.

D. RECOMMENDATIONS

The Navy's strategy for information dominance states that the information war-fighting domain is cyberspace and the network and the electromagnetic spectrum comprise that battle-space (Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet Public Affairs, 2012)." To guide its future maneuvers within the information war-fighting domain the Navy has developed three documents, which will guide Navy Information Dominance and Cyber warriors into the future. They are the Navy Strategy for Achieving Information Dominance 2013–2017, Navy Cyber Power 2020, and the Navy Information Dominance Corps Human Capital Strategy 2012–2017. Each document lays out a strategic plan that will ensure the U.S. Navy achieves information dominance by striving to maintain the operational advantage gained from fully integrating information functions, capabilities, and resources to optimize decision-making and war-fighting (Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet Public Affairs, 2012). These are not documents for the Information Dominance Corps (IDC) alone. Unrestricted line officers, and surface warfare officers in particular, need to read and understand the ID vision in order to fully integrate and employ surface ships in the struggle for information dominance.

These documents focus on the three fundamental information dominance capabilities of assured command and control, battle-space awareness, and integrated fires, and claim they set broad but achievable goals, including strong and secure U.S. Navy command and control and information dominance as a war-fighting discipline (Commander, U.S.

Fleet Cyber Command/U.S. Tenth Fleet Public Affairs, 2012). They do not however explain what exactly needs to be done, using current capabilities, to accomplish these fundamental information dominance capabilities. There is no clear definition describing what cyber means to the Navy and the Department of Defense as a whole. A definition describing what cyber is needs to be accepted. It is difficult to develop and explain strategy within a cyber-environment without this definition. The rhetoric that describes these capabilities needs to be backed up with training on which assets are best suited to support each goal and how ship commanders may fit into supporting the achievement of assured command and control, battle-space awareness and integrated fires.

A simple definition for cyber is anything relating to or involving computers or computer networks, like the Internet or World Wide Web (Merrium-Webster, 1991). This definition lends itself to define the cyber-domain as the space where computer network operations take place. This newest of domains is difficult to constrain to modern rules of engagement and civil law due to the fact that there are no truly defined nation-state borders within the cyber-domain. A strategy within this type of environment is easier to achieve if it first focuses on protecting one’s own assets before attempting to develop offensive capabilities.

Surface ships can be integrated into the goals of assured command and control and battle-space awareness through the integration of their tactical data link and EW capabilities. Ships may be the only actual eyes and ears on station to verify what a C2 center believes the situation to be, and this makes them vital to authenticating the information environment. Ships may also be used to back up these goals by ensuring they do not solely rely on the modern cyber related and IP-based computer networked technologies to run the C2 construct. Ways to train for this could include a reinvigoration of basic seamanship skills for signals to other ships and forcing a ship to function without the aid of computer chat functions and e-mail. Another important training tool would be to teach ship operators the fundamentals of information, how it may manifest itself, and how it can affect the actions of decision makers. It is not good enough to simply know how to read a radar screen or COP. The user needs to fundamentally understand how those tools function and how the information picture they are using is developed and the possibility for errors.

Ships need to be viewed as more than kinetic platforms waiting to put warheads on foreheads. The EW capabilities of a surface ship give it the ability to gather information on enemy forces, and deception capabilities provide the ability to inject false information into the information environment. Other MISO related functions could include providing print production capabilities to ally or special-forces, and enabling them to accomplish missions by proving a base of operations more robust than the equipment they are able to carry into the environment. UAVs embarked onboard a ship may be capable of disseminating deceptive information or pamphlets in support of MISO operations.

Just as the role of surface ships evolved to adjust to changes in the technology and tactics of aircraft, submarines, and missiles—the role of surface ships must continue to adapt to changes in the technology and tactics of the cyber domain and the battle for information dominance. It requires the full attention of all stakeholders to find the best methods. The IDC must think about and understand ships and their capabilities just as shipboard experts must understand the impact of information and operations in the cyber domain.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

> Control of information-much of it through the electromagnetic spectrum—is already growing more important than the control of territory in modern warfare.
>
> -Admiral Jonathan Greenert, Chief of Naval Operations, 23 September 2011

The DoD views information itself as a vital resource to mission accomplishment but does not clearly define how it will use all of the information operations tools available to achieve information dominance and while conducting operations in cyberspace. U.S. Navy assets such as the Aegis guided missile cruisers (CG) and destroyers (DDG) provide highly mobile platforms capable of carrying out multiple missions within and in support of the realm of information dominance and cyber warfare, if properly employed. They are able to carry out these missions only if those that command them understand the importance of what is at the heart of information dominance and cyber warfare; information itself and its ability to affect human behavior and influence decision making.

It is information itself that is the foundation of all action. Any foundation for attaining information dominance has to be based in the understanding of information and its effect on behavior.

Controlling the ability to access and process information and information systems faster and more effectively while denying an adversary is the goal of information dominance and serves several purposes. It can deny information availability to adversaries during important junctures in his operations. It can be used deceptively to provide false information causing an adversary to reach an incorrect conclusion. It can also degrade the confidence of adversarial decision makers have in their information systems (Poisel, 2002). The ability to attain information dominance over an adversary gives a commander almost complete control over the information environment. It is an advantage that may be a better measure for victory than a measurement of brute force or firepower.

The extensive use of modern information systems and technologies during modern conflicts and operations, such as the Global War on Terror and the Gulf Wars, has led these conflicts to be labeled as the information wars, but calling them information wars does not imply that they are the first conflicts where information was use. Using information in warfare is not a new concept, but the developments of information technologies greatly affects the way war is fought (Poisel, 2004). The capabilities of modern war ships are an example of information systems that change the way wars are fought. The ability to network information gathered from a fleet of ships into one common operating picture gives ship commanders an edge over their adversaries through enabling him or her to make decisions faster with information not available to the opposing force. Ship commanders, enabled with modern technology, need to understand how the information systems they command operate across multiple domains and the vulnerabilities they are exposed to through the reliance on those technologies. Such vulnerability is inherent in complex systems, but the benefits are of such value that accepting some risk of disruption while taking action to reduce vulnerability is warranted.

With the Navy's increasing role in information dominance there needs to be clearer instruction or doctrine on how to view and employ its surface combatants in that capacity. How will commanders understand the missions they may be tasked to accomplish regarding information dominance without clear guidance? Commanders act on what they know. The quality of what they know is based on previous experience, the information they are given, and the fidelity of the information environment.

The Navy needs to emphasize the importance of understanding information and its effect on human behavior. This understanding comes from training and education that incorporates the psychology of information; an education that is not centered on just the technology that is used to collect and interpret information.

A. RECOMMENDATIONS FOR FURTHER RESEARCH

An aspect of the information explosion that has a tremendous impact on the Navy's war fighting and humanitarian operations is the omnipresent nature of social media such as Facebook, Twitter, and blogs. Understanding how the change in information flow and availability caused by social media outlets impacts human behavior and will have meaningful consequences for military decision making. Military activities that were once isolated and difficult to observe are now exposed and broadcast instantaneously around the world. Social media and the abundance of portable, very sophisticated computers allow information to reach the far corners of the earth at near real-time (Macke, 2013). Knowledge of what is happening in military events is no longer reserved information for political elites and military commanders. If people have the ability to make a connection to cyberspace, they have the opportunity to know anything about what is going on in the world. This access complicates the application of friendly command and control, increases an enemy’s knowledge of events, and possibly enables them to execute more effective actions and reactions (Macke, 2013). Commanders need to understand how the use of social media and increased access to information outlets affects their ability to interrupt an enemy’s C2 and decision cycles.

Information is not only a powerful concept when used to make command decisions, but its critical role in society raises wider ethical issues: who owns information? Who controls its dissemination? Who has access to information (Floridi, 2010)? Further research into this area could explore how information can legally be controlled and how the increasing capability to access information may influence or affect a commander’s ability to make decisions.

LIST OF REFERENCES

American Technology Corporation. (2004). LRAD: Long range acoustic device–the sound of force protection. Retrieved October 10, 2012, from American Technology Corporation: http://www.atcsd.com

Breuer, W. (1993). ***Hoodwinking Hitler: The Normandy deception.*** Westport, CT: Praeger.

Casey-Maslen, S. (2010, October). Non-kinetic-energy weapons termed 'non-lethal'. Retrieved January 17, 2013, from Geneva-Academy: www.geneva-academy.ch/.../Non-Kinetic-EnergyOctober2010

Coakley, T. (1992). ***Command and control for war and peace.*** Washington, DC: National Defense University Press.

Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet Public Affairs. (2012, November 28). Navy's information dominance and cyber leaders sign vision documents. Retrieved January 15, 2013, from America's Navy: http://www.navy.mil/submit/display.asp?story_id=70841

Defense Industry Daily. (2011, July 19). ***U.S. Navy: from "slick 32s" to SEWIP.*** Retrieved January 9, 2013, from Defense Industry Daily: http://www.defenseindustrydaily.com/U.S.-Navy-From-Slick-32s-to-SEWIP-05365/

Department of Defense. (2012, September 4). ***DoD dictionary of military terms.*** Retrieved January 14, 2013, from Defense Technical Information Center: http://www.dtic.mil/doctrine/dod_dictionary/data/i/9718.html

Department of the Navy. (2012, November). ***Navy strategy for achieving information dominance 2013–2017.*** Washington, DC: Author.

Department of The Navy. (2013). Navy organization. Retrieved January 20, 2013, from America's Navy: http://www.navy.mil

Donald, D. (2011, November 14). Fire Scout proves its value in Middle East warzones. Retrieved January 29, 2013, from AIN Online: http://www.ainonline.com/aviation-news/dubai-air-show/2011-11-14/fire-scout-proves-its-value-middle-east-warzones

Dorsett, J. (2010, April 14). Information dominance and the U.S. Navy's cyber warfare vision. Retrieved January 26, 2013, from Defense Technical Information Center: http://www.dtic.mil/ndia/2010SET/Dorsett.pdf

Dunn, C., Powell, G., Martin, C., Hamilton, M., & Pangle, C. (2004). ***Information superiority/battle command (network centric warfare environment)***. Fort Gordon, GA: U.S. Army Battle Command Battle Lab.

Floridi, L. (2010). ***Information: a very short introduction***. Oxford: Oxford University Press.

Gehrke, K. A. (2012). ***The unexplored impact of IPv6 on intrusion detection systems***. M.S. thesis. Retrieved from Defense Technical Information Center. (ADA 561931)

Lewis, W. G., Elbourn, T. M., Schermerhorn, B. R., & Machleit, R. L. (1980, August 29). ***AN/SLQ-32(V) operator's handbook***. Retrieved January 16, 2013, from Defense Technical Information Center: http://www.dtic.mil/docs/citations/ADA090473

Lippmann, W. (1943). ***Public opinion***. New York: Macmillan.

Lundquist, E. H. (2010, July). The entire Indian Ocean is up for grabs. Retrieved January 9, 2013, from U.S. Naval Institute Proceedings: http://www.usni.org/magazines/proceedings/2010-07/entire-indian-ocean-grabs

Macke, R. (2013, January). ***Command and control: The warfighters glue***. Retrieved January 10, 2013, from U.S. Naval Institute: http://www.usni.org/magazines/proceedings/2013-01/

McConnell, L. M. (2005, February 4). Redefining combined arms in today's operational environment. Retrieved January 17, 2013, from Defense Technical Information Center: http://handle.dtic.mil/100.2/ADA507329

Merriam-Webster. (2013). Information. Retrieved January 14, 2013, from Merriam-Webster.com: http://merriam-webster.com/information

Merrium-Webster. (1991). Cyber. Retrieved January 31, 2013, from Merrium-Webster Dictionary Online: http://www.merrium-webster.com/idictionary/cyber

Naval Sea Systems Command. (2012, October 24). AEGIS. Retrieved November 07, 2012, from Navy Fact File: http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=200&ct=2

Naval Sea Systems Command. (2012, October 24). Surface electronic warfare improvement program (SEWIP). Retrieved November 18, 2012, from Navy Fact File: http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=475&ct=2

Naval War College. (2012). ***Information operations.*** Monterey, CA, USA: Author.

Navy Warfare Development Command. (2007, February). ***Navy tactical reference publication cyclone class patrol coastal ship, NTRP 3-20.6.25.*** Norfolk, VA, United States of America.

Navy Warfare Development Command. (2011). ***Multi-threat surface ship defense NTRP 3-20.3.1.*** Washington, DC: Office of the Chief of Naval Operations.

Northrop Grumman. (2011, December 6). U.S. Navy, Northrop Grumman demonstrate first manned-unmanned intel sharing. Retrieved January 29, 2013, from Northrop Grumman: http://www.irconnect.com/noc/press/pages/news_releases.html?d=240071

Northrop Grumman. (2013). MQ-8B Fire Scout. Retrieved January 29, 2013, from Northrop Grumman Aerospace Systems: http://www.as.northropgrumman.com/products/mq8bfirescout_navy/index.html

Poisel, R. (2002). ***Introduction to communication electronic warfare systems.*** Norwood, MA, USA: Artech House INC.

Poisel, R. (2004). ***Modern communications jamming principles.*** Norwood, MA: Artech House INC.

Stillions, T. (2012, October 13). SPAWAR expert discusses getting ahead of the growing cyber threat. Retrieved December 13, 2012, from Navy.mil: http://www.navy.mil/submit/display.asp?story_id=50853

SUAS News Staff. (2012, December 30). Navy issues hurry-up order to equip Fire Scout UAS with maritime surveillance radar. Retrieved January 29, 2013, from SUAS News: http://www.suasnews.com/2012/12/20410/navy-issues-hurry-up-order-to-equip-fire-scout-uas-with-maritime-surveillance-radar/

Tangredi, S. J. (2002). ***Globalization and maritime power.*** Washington, DC: Institute for National Strategic Studies.

Tsui, J. B.-y. (2005). ***Microwave receivers with EW applications.*** Raleigh, NC: Scitech Publishing INC.

U.S. Army War College. (2011). ***Information operations primer: fundamentals of information operations.*** Carlisle, PA: U.S. Army War College.

U.S. Fleet Cyber Command/U.S. Tenth Fleet. (2012, September 18). U.S. fleet cyber command/U.S. tenth fleet. Retrieved January 15, 2013, from U.S. fleet cyber command mission: http://www.public.navy.mil/fcc-c10f/Pages/usfleetcybermission.aspx

Ultra Electronica. (2011, February 28). Joint aerial layered network tactical communications system. Retrieved Jan 16, 2013, from Ultra Electronics Advanced Tactical Systems: http://ultra-ats.com

U.S. Office of the Joint Chiefs of Staff. (2007, Jan 27). Joint publication 3-13.1 electronic warfare. Washington, DC: Author.

U.S. Office of the Joint Chiefs of Staff. (2011, December 20). Joint Publication 3-13.2 military information support operations. Washington, DC: Author.

U.S. Office of the Joint Chiefs of Staff. (2012, November 27). JP 3-13 information operations. Washington, DC: Author.

USS George Washington Public Affairs. (2012). INTEL. Retrieved January 9, 2013, from USS George Washington: http://www.gw.navy.mil/core/departments/DEP%20PAGES/intel.html

Walsh, D. (2012, June 25). Demand grows for tactical unmanned aircraft. Retrieved January 29, 2013, from Defense Systems: knowledge technologies and net-enabled warfare: http://defensesystems.com/articles/2012/06/25/uas-report-small-and-medium-unmanned-aircraft.aspx

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Steve Iatrou
   Naval Postgraduate School
   Monterey, California

4. Capt Deidre McLay, USN
   Naval Postgraduate School
   Monterey, California

5. Dr. Dan C. Boger
   Naval Postgraduate School
   Monterey, California